



HEALTH AFFAIRS



HIPAA Compliance Tool: HIPAA BASICS™ Update

TMA Privacy Office

June 2005

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Agenda

- Introduction
- User Roles and Responsibilities
- Report Admin Functionality
- Enhanced Gap Analysis Details
 - Associating Gaps with a HIPAA Rule
 - Tagging Gaps for rolled up reporting
 - Requirement Notes
 - Enhanced Subscription Reporting

Training Objectives

- Upon completion of this training, you will be able to:
 - Identify use of HIPAA BASICS™
 - Describe user roles and responsibilities
 - Identify functionality of Report Admins at each level
 - Generate enhanced reporting as a Report Admin, Subscriber Admin, and Lead User
 - Identify enhanced Gap Analysis details

Introduction

- Target Audience: Individuals assigned Report Admin responsibility for using HIPAA BASICS™ for tracking HIPAA Compliance
- Length of Training:
 - 30 minutes

Use of HIPAA BASICS™

- MHS HIPAA Security Integrated Project Team (IPT) is responsible for developing and executing the strategy for implementation and maintenance of the HIPAA Security Rule requirements throughout DoD
- MHS must be able to establish an initial baseline and track progress toward compliance with HIPAA Security requirements
 - Report on the state of MHS HIPAA Security at any point
- TMA Privacy Office has provided HIPAA BASICS™ to track and document compliance with HIPAA Privacy and Security Rules
- Mandated for HIPAA Security on April 27, 2004
- Strongly recommended for HIPAA Privacy

What is HIPAA BASICS™

- HIPAA BASICS™ is:
 - A web-based application
 - Used to collect, store, process data, and generate reports on HIPAA requirements
 - Assists you in identifying where compliance gaps exist and provides suggested compliance activities relating to HIPAA Administrative Simplification
- Accessible at hipaacompliance.tricare.osd.mil

User Roles and Responsibilities

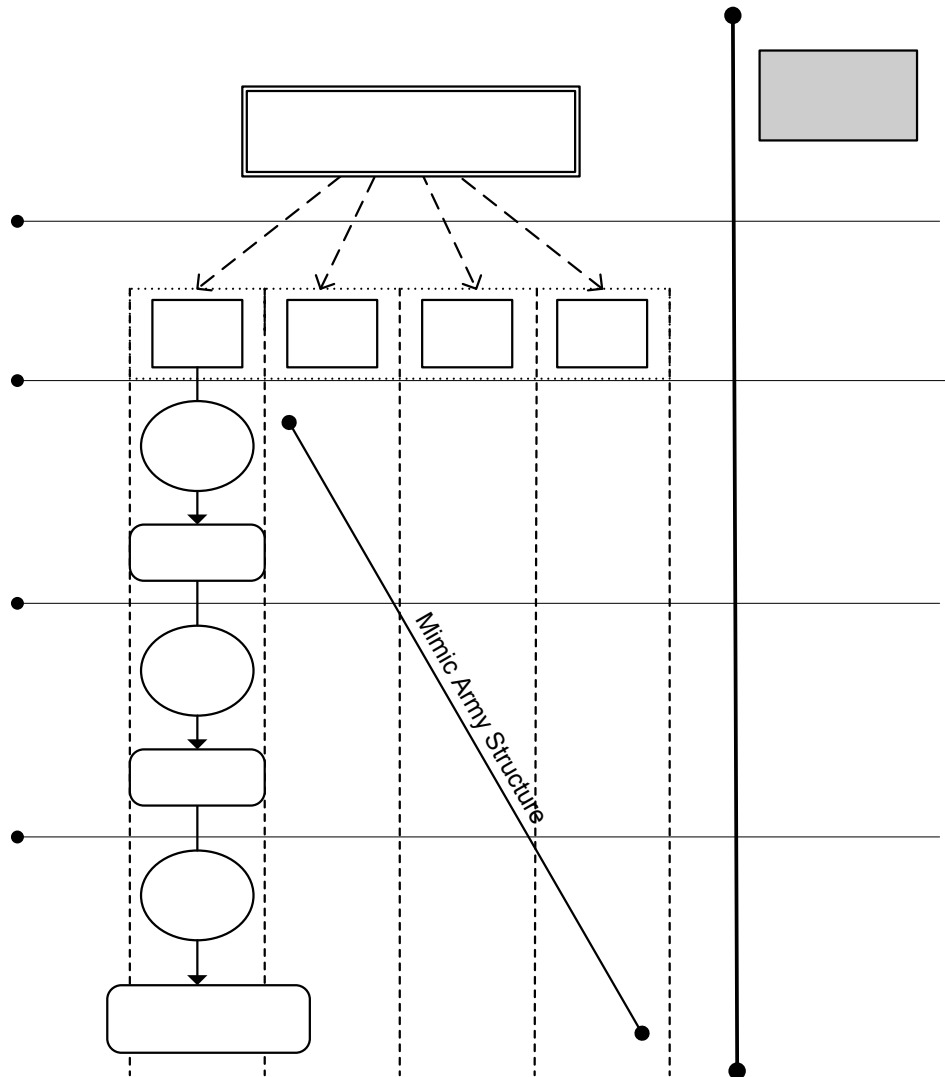
Roles and Responsibilities

Objectives

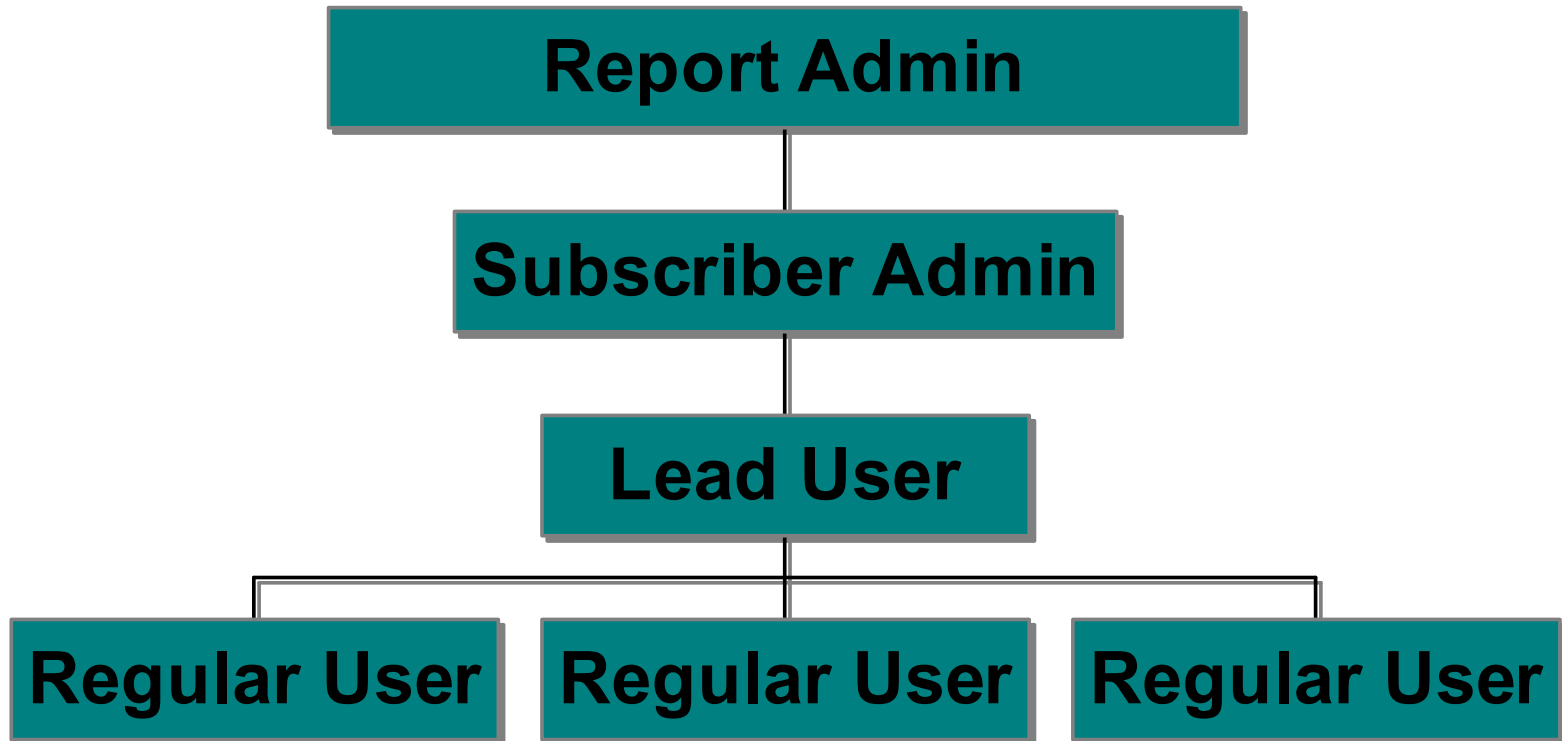
- Upon completion of this lesson, you will be able to:
 - Describe the structure of subscriptions within HIPAA BASICS™
 - Identify users roles and responsibilities associated with:
 - Report Admin
 - Subscriber Administrator
 - Lead User
 - Regular User

Roles and Responsibilities

High Level Hierarchy



Subscription Structure



Roles and Responsibilities

User Roles within HIPAA BASICS™

- **Report Admins** are typically Privacy and Security Officers who are assigned the responsibility of generating rolled up compliance reporting
- **Subscriber Administrators** should be someone with an appropriate level of security clearance or access, preferably someone with a high level of comfort with technology, such as an IT professional
- **Lead Users** are generally high level managers, such as the Compliance Officer or Privacy/Security Officer
- **Regular Users** are the Subject Matter Experts (SMEs) in areas such as Medical Records

Roles and Responsibilities

Report Admin Functions

- Run reports for organizations within their hierarchy (rolled up reporting)
- View profiles for Report Admins at the same level
- Ability to update profiles for subordinate Report Admins
- Login to Subscriptions
- Can have up to three Report Admins for each organization

Subscriber Administrator Functions

- Manage the tool administratively
- Create and edit user accounts within subscription
- View and edit all Gap Analysis across the subscription
- Add Gap Analysis for Lead Users within subscription
- Reassign Lead Users to Gap Analysis within subscription

Roles and Responsibilities

Lead User Functions

- Manage compliance assessments
- Add members to a compliance assessment team
- Remove members from a compliance assessment team
- Assign requirements to team members
- Run reports and generate project plans
- Edit information related to their compliance assessments
- Download Policy and Form templates
- Assign gaps to a HIPAA rule
- Select gaps for rolled up reporting

Regular User Functions

- Address specific requirements to determine compliance
- View the work of other team members, however...
 - Can only answer requirement questions that are assigned to them by the Lead User

Roles and Responsibilities

User Roles and Responsibilities Summary

- You should now be able to:
 - Understand the structure of subscriptions within HIPAA BASICS™
 - Identify users roles and responsibilities associated with:
 - Report Admin
 - Subscriber Administrator
 - Lead User
 - Regular User

Report Admin Functionality

Report Admin Functionality

Objectives

- Upon completion of this lesson, you will be able to:
 - Identify functionality of Report Admins at each level
 - Describe the Report Admin interface
 - Generate High Level and Detailed Requirement Reports

Chart of Report Admin Functionality

<u>Function</u>	<u>Level 0</u>	<u>Level 1</u>	<u>Level 2</u>	<u>Level 3</u>
High Level Summary	x	x	x	x
Detailed Requirement Report			x	x
View RA profiles on same level	x	x	x	x
Update subordinate RA profiles	x	x	x	x
View filtered Subscription lists		x	x	x
Sub Admin Subscription login			x	x

Obtaining an Account

- Report Admin accounts are created by the HIPAA Support Center
 - An approved request for a Report Admin to be created must be routed to the HIPAA Support Center by the Service Representative, via the appropriate chain of command
 - Service Representatives must email the approved request to: hipaasupport@tma.osd.mil
- The HIPAA Support Center will email the appropriate Report Admin login information to the designated individual

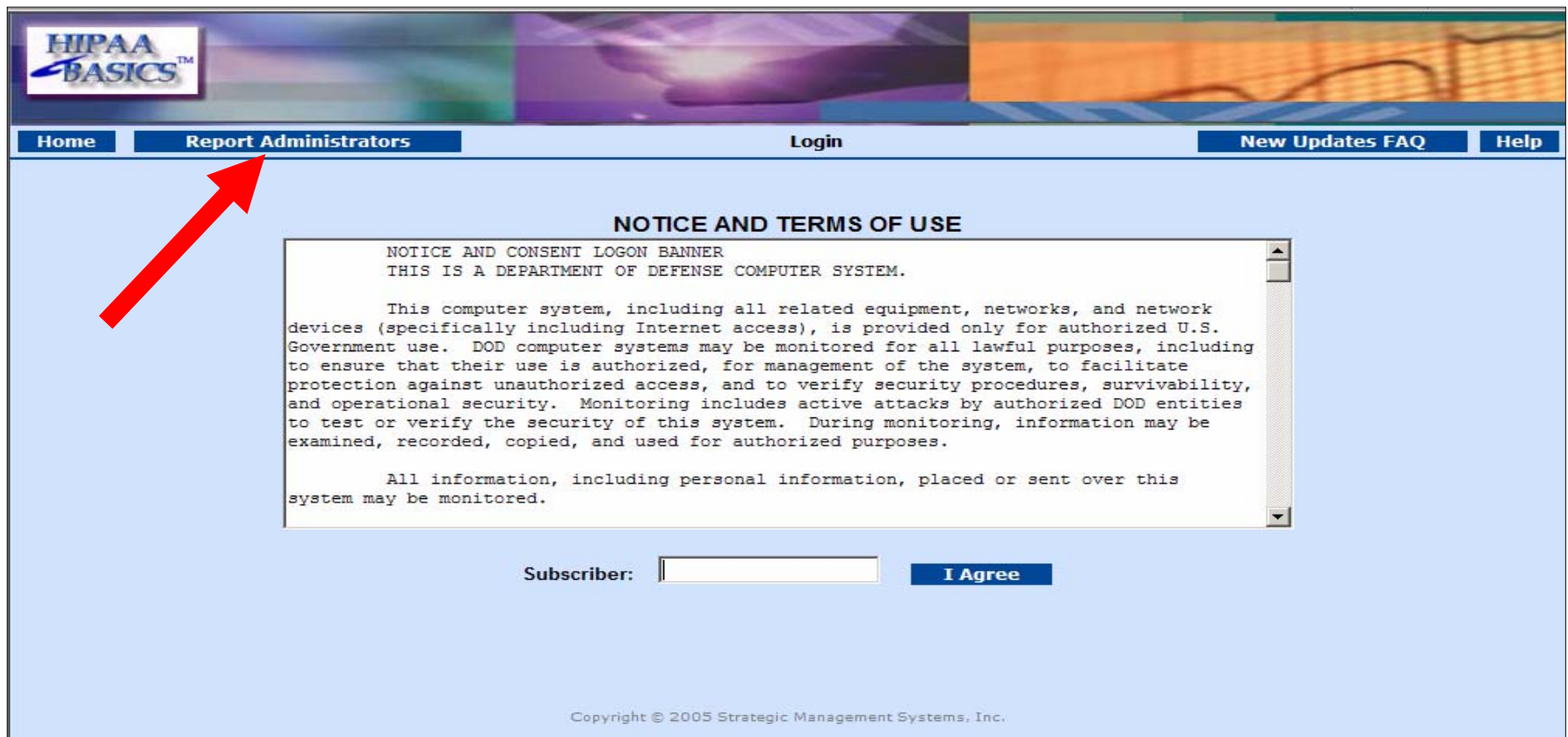
Report Admin Login Information

- There are three pieces of information that must be known in order to login:
 - Organization
 - Report User ID
 - Password
- Upon logging in for the first time you will be prompted to change your password
- Passwords must meet the DoD requirements (refer to User Guide)

Report Admin Functionality

Report Admin Login (1 of 3)

1. Enter URL: hipaacompliance.tricare.osd.mil
2. Click on **Report Administrators** button



The screenshot shows the HIPAA Basics website interface. At the top left is the 'HIPAA BASICS' logo. A navigation bar contains buttons for 'Home', 'Report Administrators', 'Login', 'New Updates FAQ', and 'Help'. A red arrow points to the 'Report Administrators' button. Below the navigation bar is a 'NOTICE AND TERMS OF USE' section. This section contains a 'NOTICE AND CONSENT LOGON BANNER' with the text: 'THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including Internet access), is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.' Below the notice is a 'Subscriber:' label, an empty text input field, and an 'I Agree' button. At the bottom of the page, the copyright notice 'Copyright © 2005 Strategic Management Systems, Inc.' is displayed.

HIPAA BASICS™

Home Report Administrators Login New Updates FAQ Help

NOTICE AND TERMS OF USE

NOTICE AND CONSENT LOGON BANNER
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM.

This computer system, including all related equipment, networks, and network devices (specifically including Internet access), is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes.

All information, including personal information, placed or sent over this system may be monitored.

Subscriber: **I Agree**

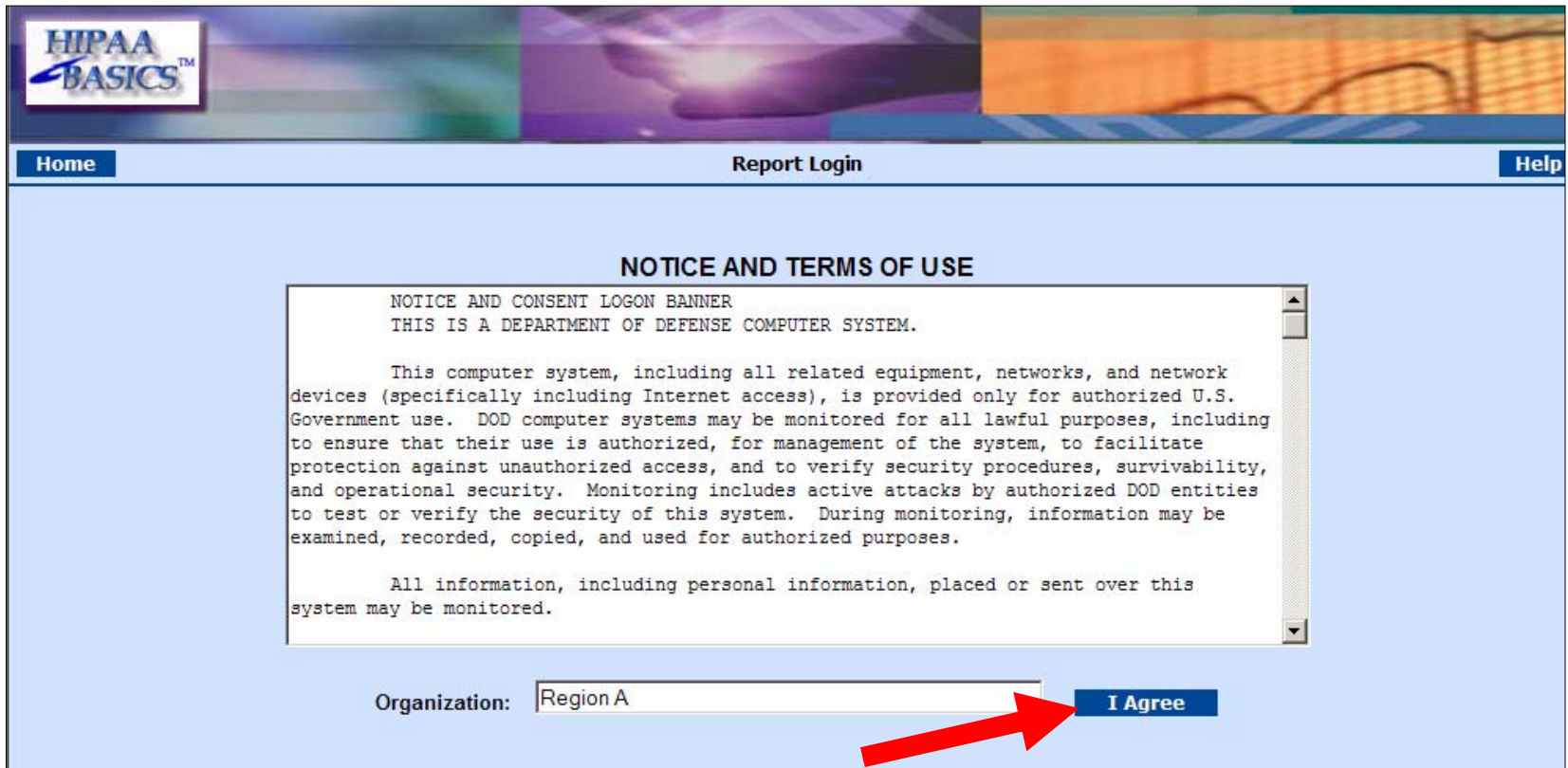
Copyright © 2005 Strategic Management Systems, Inc.

Report Admin Functionality

Report Admin Login (2 of 3)

3. Enter Organization

4. Click on **I Agree**



The screenshot displays the 'Report Admin Login' interface. At the top left is the 'HIPAA BASICS™' logo. The navigation bar includes 'Home', 'Report Login', and 'Help'. The main content area features a 'NOTICE AND TERMS OF USE' section with a scrollable text box containing the following text:

NOTICE AND CONSENT LOGON BANNER
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM.

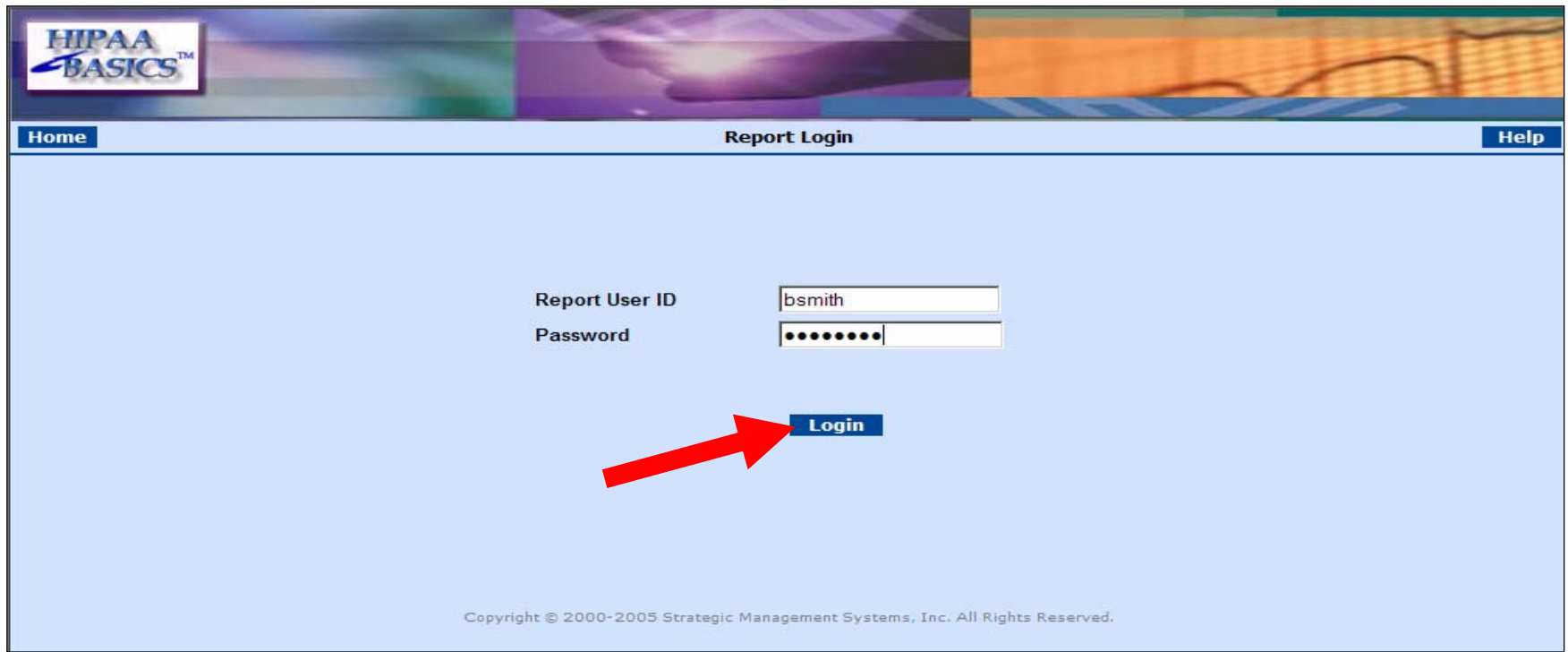
This computer system, including all related equipment, networks, and network devices (specifically including Internet access), is provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes.

All information, including personal information, placed or sent over this system may be monitored.

Below the notice, there is an 'Organization:' label followed by a text input field containing 'Region A'. To the right of the input field is a blue button labeled 'I Agree'. A red arrow points from the bottom center towards the 'I Agree' button.

Report Admin Login (3 of 3)

5. Enter Report User ID and Password
6. Click on [Login](#)



HIPAA BASICS™

Report Login

Home **Help**

Report User ID: bsmith

Password: ••••••••

Login

Copyright © 2000-2005 Strategic Management Systems, Inc. All Rights Reserved.

Report Admin Functionality

Report Admin Menu



Report Admin Menu

- High Level Summary Report
 - Generate high level summary report for any subscription within their hierarchy
- Detailed Requirement Report
 - Generate detailed requirement report for any subscription within their hierarchy
- Subscriber List
 - View list of Subscriptions within the hierarchy
- Report Users
 - View and update report user profiles within the hierarchy

High Level Summary Report (1 of 5)

- New report developed to facilitate overall reporting at each level of the organization
 - Reports by completion of tasks and requirements
- Shows an overview of HIPAA Compliance efforts
- Available in both graphical and table format
- Can be run by Subscriber Administrators, Lead Users, and Report Admins
- Can only be generated for Gaps that have been assigned a HIPAA Rule and are tagged
- Report Admins are able to generate a rolled up report for all subordinates in their hierarchy

High Level Summary Report (2 of 5)

1. Click on **High Level Summary Report** button



Report Admin Functionality

High Level Summary Report (3 of 5)

2. Click on List Sub-Groups button

The screenshot shows the 'High Level Summary Report' interface. At the top left is the 'HIPAA BASICS™' logo. To the right, it displays 'Organization : Region A' and 'User : Bob Smith'. Below this is a navigation bar with 'Log Off', 'Menu', 'High Level Summary Report', and 'Help' buttons. The main content area contains instructions: 'Select report options and click "HTML Report" or "XLS Report" to build a report. Click "List Sub-Groups >>" to view or build a report based on the selected subordinate organizations.' A red arrow points to the 'List Sub-Groups >>' button. Below the instructions, there is a section 'Include the following in Report:' with the following options: 'Select HIPAA Rule:' with a dropdown menu showing 'Standards for Electronic Transactions and Code Sets'; 'Report Style:' with radio buttons for 'Tabular' (selected) and 'Graphical'; 'Requirement Compliance Status' with a checked checkbox; 'Requirement Task Status' with a checked checkbox; and 'Non-Applicable Tasks' with an unchecked checkbox. At the bottom, there are two buttons: 'HTML Report' and 'XLS Report'. A checkbox for 'Graphical Report Display Totals' is also present.

HIPAA BASICS™

Organization : Region A
User : Bob Smith

Log Off **Menu** **High Level Summary Report** **Help**

Select report options and click "HTML Report" or "XLS Report" to build a report. Click "List Sub-Groups >>" to view or build a report based on the selected subordinate organizations.

List Sub-Groups >>

Include the following in Report:

Select HIPAA Rule: Standards for Electronic Transactions and Code Sets

Report Style: ☒ Tabular ☐ Graphical

☒ Requirement Compliance Status ☒ Requirement Task Status ☐ Non-Applicable Tasks

☒ Graphical Report Display Totals

HTML Report **XLS Report**

High Level Summary Report (4 of 5)

- Select the [Organization](#) link to drill down within your hierarchy
3. Select reporting organizations

Log Off		Menu		High Level Summary Report		Help	
<< Hide Sub-Groups							
Sub-Groups							
Select	Organization						
<input checked="" type="checkbox"/>	MTF A						
<input checked="" type="checkbox"/>	MTF B						
<input type="checkbox"/>	MTF C						
Include the following in Report:							
Select HIPAA Rule:	<div>Standards for Electronic Transactions and Code Sets</div>						
Report Style:	<input checked="" type="radio"/> Tabular <input type="radio"/> Graphical						
<input checked="" type="checkbox"/> Requirement Compliance Status	<input checked="" type="checkbox"/> Requirement Task Status				<input type="checkbox"/> Non-Applicable Tasks		
<input checked="" type="checkbox"/> Graphical Report Display Totals							
HTML Report				XLS Report			

High Level Summary Report (5 of 5)

4. Select HIPAA Rule
5. Select Report style and details
6. Click HTML Report or XLS Report

Log Off Menu High Level Summary Report Help

<< Hide Sub-Groups

Sub-Groups

Select	Organization
<input checked="" type="checkbox"/>	MTF A
<input checked="" type="checkbox"/>	MTF B
<input type="checkbox"/>	MTF C

include the following in Report:

Select HIPAA Rule: Security Standards

Report Style: ☒ Tabular ☐ Graphical

☒ Requirement Compliance Status ☒ Requirement Task Status ☒ Non-Applicable Tasks

☒ Graphical Report Display Totals

HTML Report XLS Report

High Level Summary Report- Tabular (1 of 2)

High Level Summary Report

Organization Name and User	Report Date	HIPAA Rule
Region A (Bob Smith)	6/15/2005	Security Standards

Reporting Organizations: MTF A; MTF B

Non-Tagged Subscriptions: none

Summary Totals

	% Compliant	% Not Compliant	# Requirements	# Compliant	# Not Compliant		
Requirement Status	16.42	83.58	134	22	112		
	% Complete	% Not Complete	% Not Answered	# Tasks	# Complete	# Not Complete	# Not Answered
Requirement Task Status	15.75	0	84.25	1651	260	0	1391
	% Non Applicable		Total # Tasks		# Non Applicable		
Non-Applicable Task Status	7.14		1778		127		

MTF A

High Level Summary Report- Tabular (2 of 2)

MTF A

	% Compliant	% Not Compliant	# Requirements	# Compliant	# Not Compliant		
Requirement Status	19.4	80.6	67	13	54		
	% Complete	% Not Complete	% Not Answered	# Tasks	# Complete	# Not Complete	# Not Answered
Requirement Task Status	18.8	0	81.2	803	151	0	652
	% Non Applicable		Total # Tasks		# Non Applicable		
Non-Applicable Task Status	9.67		889		86		

MTF B

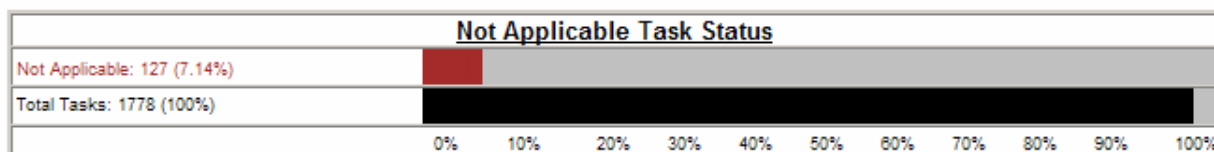
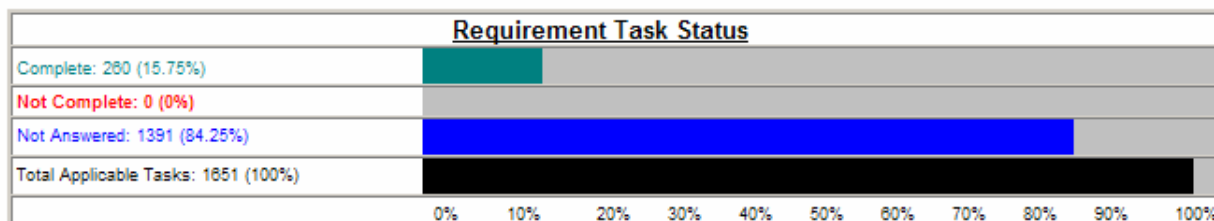
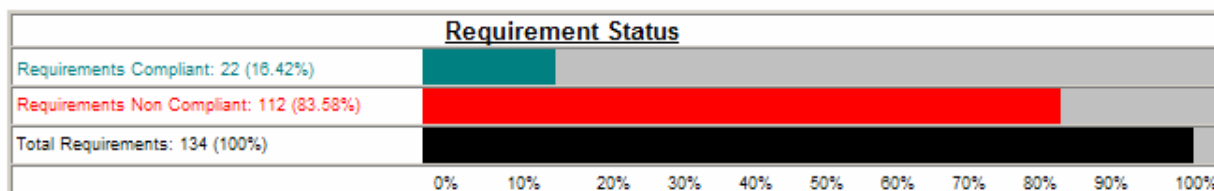
	% Compliant	% Not Compliant	# Requirements	# Compliant	# Not Compliant		
Requirement Status	13.43	86.57	67	9	58		
	% Complete	% Not Complete	% Not Answered	# Tasks	# Complete	# Not Complete	# Not Answered
Requirement Task Status	12.85	0	87.15	848	109	0	739
	% Non Applicable		Total # Tasks		# Non Applicable		
Non-Applicable Task Status	4.61		889		41		

High Level Summary Report – Graphical

High Level Graphical Report

Organization Name and User	Report Date	HIPAA Rule
Region A (Bob Smith)	6/15/2005	Security Standards

Reporting Organizations: MTF A; MTF B
Non-Tagged Subscriptions: none

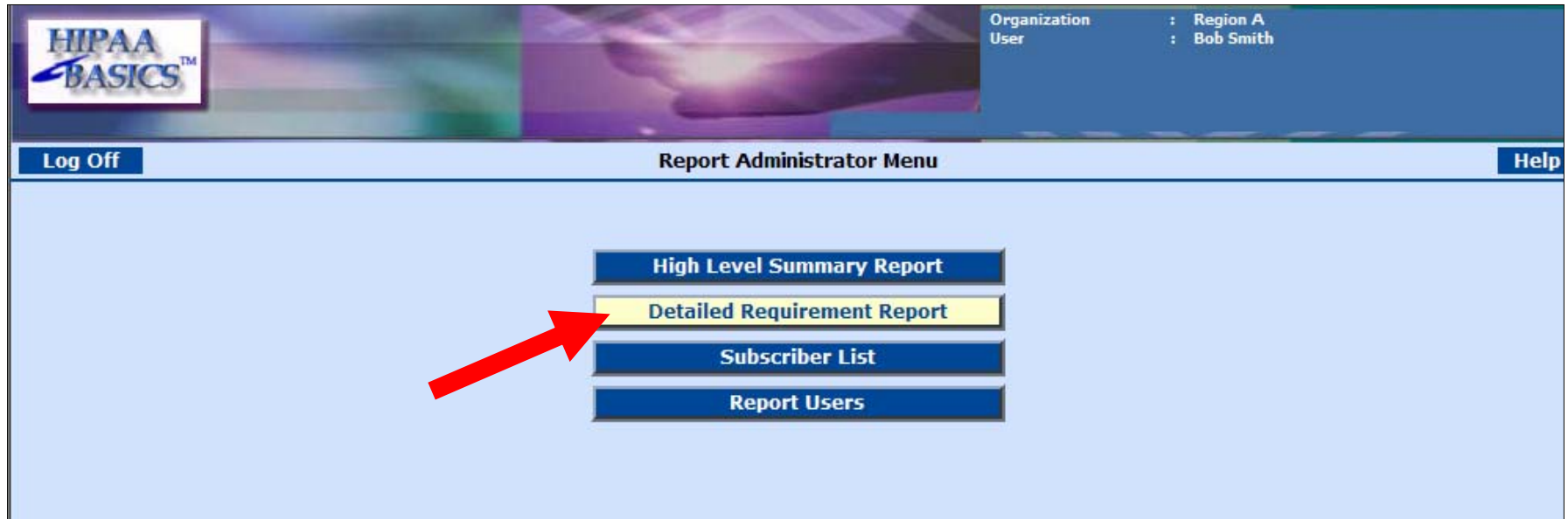


Detailed Requirement Report (1 of 3)

- Newly developed to show detailed compliance efforts at each level of an organization
- Shows a breakdown of the level of compliance for all requirements and tasks
- Can only be generated for Gaps that have been assigned a HIPAA Rule and are tagged
- Can be run by Subscriber Administrators, Lead Users, and Report Admins
- Report Admins are able to generate a rolled up report for all subordinates in their hierarchy
- Available in HTML or Excel

Detailed Requirement Report (2 of 3)

1. Click on the Detailed Requirement Report button



Detailed Requirement Report (3 of 3)

2. After selecting reporting organizations, Select the HIPAA Rule and report style
3. Click on [HTML Report](#) or [XLS Report](#)

Log Off		Menu		Detailed Requirement Report		Help	
Sub-Groups							
Select	Organization						
<input checked="" type="radio"/>	MTF A						
<input type="radio"/>	MTF B						
<input type="radio"/>	MTF C						
Include the following in Report:							
Select HIPAA Rule:		<input type="text" value="Security Standards"/>					
<input checked="" type="checkbox"/> Requirement Question	<input checked="" type="checkbox"/> # Tasks Complete	<input checked="" type="checkbox"/> # Tasks Not Complete					
<input checked="" type="checkbox"/> # Tasks Not Answered	<input checked="" type="checkbox"/> # Tasks Not Applicable	<input checked="" type="checkbox"/> Requirement Note					
<input checked="" type="radio"/> All <input type="radio"/> Compliant Requirements <input type="radio"/> Non-Compliant Requirements							
HTML Report				XLS Report			

Report Admin Functionality

Detailed Requirement Report Results

Detailed Requirement Report

Organization Name and User	Report Date	HIPAA Rule
Region A (Bob Smith)	6/15/2005	Security Standards

Reporting Organization: MTF A
Non-Tagged Subscriptions: none

Req#	Req Question	Organization	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliant
107	A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.	Training	100	20	0	0	0	20	N	N
Req#	Req Question	Organization	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliant
108	A Risk Analysis to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI was conducted (R).	Training	100	19	0	0	0	19	Y	Y
Req#	Req Question	Organization	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliant
109	A Risk Management Process that implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level is in place (R).	Training	100	14	0	0	0	14	N	N
Req#	Req Question	Organization	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliant
110	A Sanction Policy to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures has been developed (R).	Training	100	7	0	0	0	7	Y	Y
Req#	Req Question	Organization	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliant
111	Information System Activity Review procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports, are implemented (R).	Training	-	0	0	0	15	15	Y	Y

Report Admin Functionality

Summary

- You should now be able to:
 - Identify functionality of Report Admins at each level
 - Describe the Report Admin interface
 - Generate High Level and Detailed Requirement Reports

Enhanced Gap Analysis Details

Enhanced Gap Analysis Details

Objectives

- Upon completion of this lesson, you will be able to:
 - Identify naming convention for Gaps
 - Assign Gaps to a HIPAA Rule
 - Tag Gaps for reporting
 - Describe importance of requirement notes
 - Generate enhanced reports at the Subscription level

Enhanced Gap Analysis Details

Naming Convention

- Naming convention for Security Gaps:
 - Baseline Security MTF
 - Active Security MTF*
 - Security Q105 MTF

Assigning Gaps to a HIPAA Rule (1 of 3)

- Associates a Gap to a HIPAA Rule (Privacy or Security)
- Once assigned a HIPAA Rule, all other rules default to not-applicable
- All menus will default to the assigned HIPAA Rule
 - Eliminates sorting
- Current Gaps in the system have not been assigned a HIPAA Rule
 - Lead Users or Subscriber Administrators will need to assign Gaps as appropriate
- Gaps must be assigned to a HIPAA Rule for reporting purposes

Enhanced Gap Analysis Details

Assigning Gaps to a HIPAA Rule (2 of 3)

1. Click on the **Add Gap** button

The screenshot displays the HIPAA BASICS web application interface. At the top, there is a header with the 'HIPAA BASICS' logo on the left and a 'Subscriber : Training' status on the right. Below the header is a navigation bar with buttons for 'Log Off', 'Back', 'Gap Analysis Project List', 'Info', 'Contact Us', and 'Help'. On the left side, there is a vertical menu with buttons for 'Users', 'Gap Analysis Project List', 'Policies & Forms', 'Add Gap', 'High Level Summary Report', and 'Detailed Report'. A red arrow points to the 'Add Gap' button. The main content area is titled 'Baseline Administrative Simplification Integrated Compliance Solution' and contains a table with the following columns: Answer, Assign, Data Collection Date, Gap ID, Rel, Report Tag, Edit, Report, and Status. The table lists several training-related gap analysis entries.

Answer	Assign	Data Collection Date	Gap ID	Rel	Report Tag	Edit	Report	Status
TRAINING	Kevin York		1489	4	N			
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING	4	N	Edit	Report	Status
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING Version 2	4	N	Edit	Report	Status
TRAINING	Subscriber Administrator	5/14/2004	DEMO GAP	4	N			
TRAINING	Subscriber Administrator	2/17/2004	DEMO GAP PREVIOUS VERSION	3	N			
TRAINING	Megan McCarron	2/27/2004	Training TEST	4	N	Edit	Report	Status

Enhanced Gap Analysis Details

Assigning Gaps to a HIPAA Rule (3 of 3)

- Select the HIPAA Rule that the Gap is associated with

[Log Off](#) [Back](#) Add New Gap Analysis Project [Help](#)

*Lead User	Megan McCarron
Data Collection Date (mm/dd/yyyy)	04/28/2005
Gap ID	TRNG Test
Notes for Client	<div></div>
Date Completed (mm/dd/yyyy)	<div></div>
Internal	<div></div>
HIPAA Rule Please select the HIPAA rule this GAP is associated with. If this GAP is being used for training or testing purposes, and will not be used for rolled up reporting, please leave the selection blank.	Security Standards
Partial Gap Analysis (OPTIONAL): If you wish to set HIPAA Rule(s) as Not Applicable, you may uncheck the corresponding Applicability boxes and thereby pre-answer with "Does Not Apply". This has the effect that the Status of all Tasks for the Requirements of the deselected Rule(s) are set to "Does Not Apply".	Applicability
Standards for Electronic Transactions and Code Sets	<input type="checkbox"/>
Standard Unique Health Identifier for Health Care Providers	<input type="checkbox"/>
Security Standards	<input checked="" type="checkbox"/>
Standards for the Privacy of Individually Identifiable Health Information	<input type="checkbox"/>
National Standard Employer Identifier	<input type="checkbox"/>
National Standard Health Plan Identifier	<input type="checkbox"/>

[Clear](#) [NewVersion](#) [Add](#)

Tagging Gaps for Reporting (1 of 4)

- Gap Analysis that will be included in rolled up reporting must be tagged by the Lead User
- A Gap Analysis must be assigned a HIPAA Rule before it can be tagged for reporting
- Only one Gap Analysis per HIPAA Rule can be tagged for reporting

Enhanced Gap Analysis Details

Tagging Gaps for Reporting (2 of 4)

- Prior to Tagging Gaps for Reporting

The screenshot displays the HIPAA BASICS web application interface. At the top, there is a header with the HIPAA BASICS logo and a subscriber selection dropdown currently set to 'Training'. Below the header is a navigation bar with 'Log Off', 'Back', 'Gap Analysis Project List', 'Info', 'Contact Us', and 'Help' buttons. A left sidebar contains a menu with 'Users', 'Gap Analysis Project List' (selected), 'Policies & Forms', 'Add Gap', 'High Level Summary Report', and 'Detailed Report'. Below the menu, the user 'Megan McCarron' is logged in. The main content area is titled 'Baseline Administrative Simplification Integrated Compliance Solution' and contains a table of gap analysis projects. The table has columns for Answer, Assign, Data Collection Date, Gap ID, Rel, Report Tag, Edit, Report, and Status. The 'Report Tag' column is highlighted with a red box. The table lists several gaps, including 'Baseline Security TRAINING' and 'DEMO GAP'.

Answer	Assign	Data Collection Date	Gap ID	Rel	Report Tag	Edit	Report	Status
TRAINING	Kevin York		1489	4	N			
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING	4	N	Edit	Report	Status
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING Version 2	4	N	Edit	Report	Status
TRAINING	Subscriber Administrator	5/14/2004	DEMO GAP	4	N			
TRAINING	Subscriber Administrator	2/17/2004	DEMO GAP PREVIOUS VERSION	3	N			
TRAINING	Megan McCarron	2/27/2004	Training TEST	4	N	Edit	Report	Status
TRAINING	Megan McCarron	4/28/2005	TRNG Test	4	N	Edit	Report	Status

Enhanced Gap Analysis Details

Tagging Gaps for Reporting (3 of 4)

1. Select **Edit** from the Gap Analysis Project List screen
2. Check the box for Reporting Tag
3. Click **Update**

HIPAA BASICS™

Please click on Add/Update to save changes...

Log Off **Back** **Edit Gap Analysis** **Help**

Data Collection Date (mm/dd/yyyy) 4/28/2005

Target Completion (mm/dd/yyyy)

Project Start (mm/dd/yyyy)

Gap ID TRNG Test

Gap Active ☒

Date Completed (mm/dd/yyyy)

Notes for Client

Internal

HIPAA Rule
Please select the HIPAA Rule this GAP is associated with. If this GAP is being used for training or testing purposes, and will not be used for rolled up reporting, please leave the selection blank.

Reporting Tag ☒


Security Standards

Project Plan **Project Plan XLS** **Reassign User Assignments** **Update**

Enhanced Gap Analysis Details

Tagging Gaps for Reporting (4 of 4)

- Report Tag column will identify Gaps that are tagged for reporting



Subscriber : Training

Log OffBack

Gap Analysis Project ListInfoContact UsHelp

Users

Gap Analysis Project List

Policies & Forms

Add Gap

High Level Summary Report

Detailed Report

Megan McCarron

Answer	Assign	Data Collection Date	Gap ID	Rel	Report Tag	Edit	Report	Status
TRAINING	Megan McCarron	4/28/2005	TRNG Test	4	Y	Edit	Report	Status
TRAINING	Kevin York		1489	4	N			
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING	4	N	Edit	Report	Status
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING Version 2	4	N	Edit	Report	Status
TRAINING	Subscriber Administrator	5/14/2004	DEMO GAP	4	N			
TRAINING	Subscriber Administrator	2/17/2004	DEMO GAP PREVIOUS VERSION	3	N			
TRAINING	Megan McCarron	2/27/2004	Training TEST	4	N	Edit	Report	Status

Requirement Notes (1 of 3)

- Requirement Notes are mandatory
- Users must enter a Requirement Note for each requirement in order to be compliant
- Red text indicating a Requirement Note has not been entered will appear on the Requirement Task screen

Enhanced Gap Analysis Details

Requirement Notes (2 of 3)

- Red text indicates that a Requirement Note is missing

1. Select **Requirement Question** link to enter a note

Log Off		Menu		Back		Requirement Tasks		Help	
HIPAA Rule		Security Standards							
Functional Area		Information Technology							
Project Category		VI: Security Management Process							
Requirement Question		107: A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.							
Regulatory Authority		A covered entity must implement Administrative Safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits. The safeguards must protect against reasonably anticipated threats or hazards to the security and integrity of such information. They must also protect against any reasonably anticipated uses and disclosures of such information that are not permitted or required. The approach is flexible. In deciding which security measures to use, a covered entity must take into account a variety of factors, including size, complexity and capabilities of the covered entity, cost, technical infrastructure and capabilities, and probability and criticality of potential risks. [164.308 (a)(1)(i); in accordance with § 164.306(a)(b)] [For exact quotation of Regulatory Authority and the Rule, see http://aspe.hhs.gov/admsimp]							
Requirement Intro		Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. An implementation requirement standard of the administrative safeguards includes a documented and well communicated Security Management Process is important as it enforces the formal analysis and assessment of risks as well as audits and sanctions. Being informed and prepared is critical for success. The security management process accomplishes this in an ever-changing security risk environment. Security standards establish a minimum level of security that covered entities must meet.							
<p>A Requirement Note for the specific Requirement is missing. The Requirement will not be considered <u>compliant</u> or <u>complete</u> until all applicable tasks are Complete and a Requirement Note has been entered.</p>									
Update					Assigned to : Megan McCarron				
ID	Status	Requirement Test						Applicability	
<input type="checkbox"/> All Complete / Not Complete		<input type="radio"/> Applicable <input type="radio"/> Not Applicable <input checked="" type="radio"/> All						<input checked="" type="checkbox"/> On / Off	
107.01	Not Answered	The administrative policies and procedures used to meet this requirement are documented.						<input checked="" type="checkbox"/>	
107.02	Not Answered	The principle of least privilege is addressed. [OPTIONAL]						<input checked="" type="checkbox"/>	
107.03	Not Answered	Separation of duties is addressed. [OPTIONAL]						<input checked="" type="checkbox"/>	
107.04	Not Answered	The required qualifications for each security management role are included. [OPTIONAL]						<input checked="" type="checkbox"/>	

Enhanced Gap Analysis Details

Requirement Notes (3 of 3)

2. Enter a Requirement Note
3. Click on **Update**

HIPAA BASICS™
Please click on Add/Update to save changes...

Log Off **Menu** **Back** **Requirement Notes** **Help**

HIPAA Rule Security Standards
Functional Area Information Technology
Project Category VI: Security Management Process
Requirement Question 107: A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.
Regulatory Authority A covered entity must implement Administrative Safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits. The safeguards must protect against reasonably anticipated threats or hazards to the security and integrity of such information. They must also protect against any reasonably anticipated uses and disclosures of such information that are not permitted or required. The approach is flexible. In deciding which security measures to use, a covered entity must take into account a variety of factors, including size, complexity and capabilities of the covered entity, cost, technical infrastructure and capabilities, and probability and criticality of potential risks. [164.308 (a)(1)(i); in accordance with § 164.306(a) (b)] [For exact quotation of Regulatory Authority and the Rule, see <http://aspe.hhs.gov/admsimp>]
Requirement Intro Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. An implementation requirement standard of the administrative safeguards includes a documented and well communicated Security Management Process is important as it enforces the formal analysis and assessment of risks as well as audits and sanctions. Being informed and prepared is critical for success. The security management process accomplishes this in an ever-changing security risk environment. Security standards establish a minimum level of security that covered entities must meet.

Requirement Notes

Requirement compliant with policies and procedures.

Update

Enhanced Gap Analysis Details

Enhanced Subscription Reporting

- High Level Summary
- Detailed Requirement Report



Subscriber : Training

Log OffBack

Gap Analysis Project ListInfoContact UsHelp

Baseline Administrative Simplification Integrated Compliance Solution

Answer	Assign	Data Collection Date	Gap ID	Rel	Report Tag	Edit	Report	Status
TRAINING	Megan McCarron	4/28/2005	TRNG Test	4	Y	Edit	Report	Status
TRAINING	Kevin York		1489	4	N			
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING	4	N	Edit	Report	Status
TRAINING	Megan McCarron	7/7/2004	Baseline Security TRAINING Version 2	4	N	Edit	Report	Status
TRAINING	Subscriber Administrator	5/14/2004	DEMO GAP	4	N			
TRAINING	Subscriber Administrator	2/17/2004	DEMO GAP PREVIOUS VERSION	3	N			
TRAINING	Megan McCarron	2/27/2004	Training TEST	4	N	Edit	Report	Status

Users

Gap Analysis Project List

Policies & Forms

Add Gap

High Level Summary Report

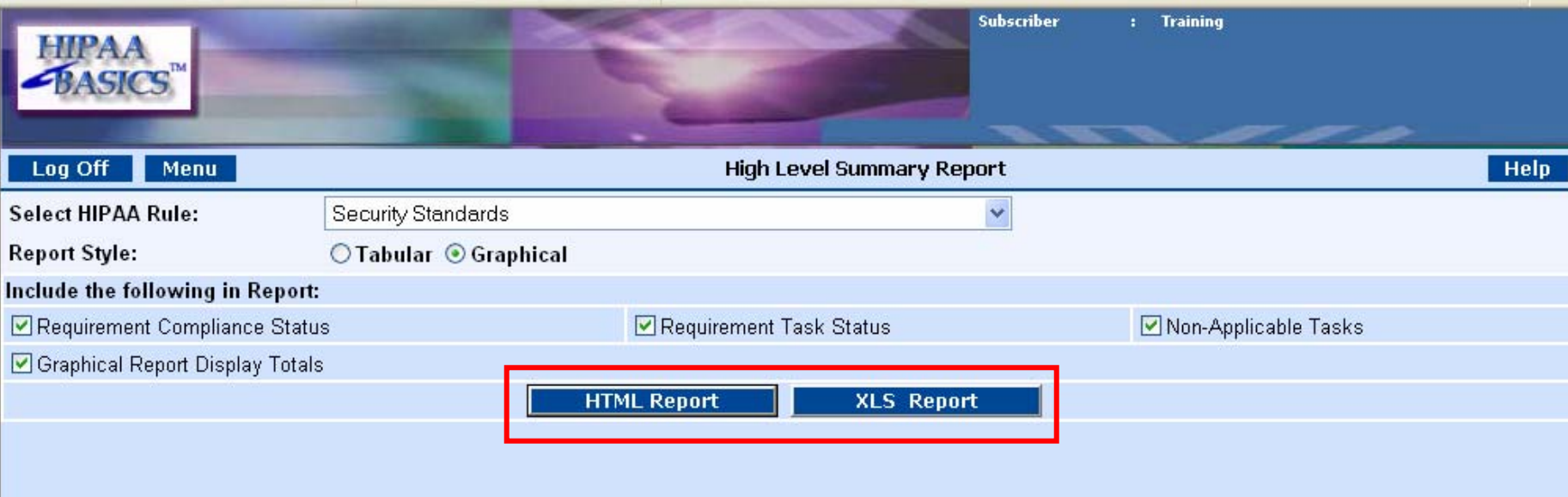
Detailed Report

[Megan McCarron](#)

Enhanced Gap Analysis Details

High Level Summary Report

1. Select HIPAA Rule and Report Style
2. Click on **HTML Report** or **XLS Report**



HIPAA BASICS™

Subscriber : Training

[Log Off](#) [Menu](#) **High Level Summary Report** [Help](#)

Select HIPAA Rule: Security Standards

Report Style: ☐ Tabular ☒ Graphical

Include the following in Report:

☒ Requirement Compliance Status ☒ Requirement Task Status ☒ Non-Applicable Tasks

☒ Graphical Report Display Totals

HTML Report **XLS Report**

High Level Summary Report- Tabular

High Level Summary Report

Organization Name and User	Report Date	HIPAA Rule
Training (Megan McCarron)	5/25/2005	Security Standards

Gap ID: TRNG Test

Lead User: Megan McCarron

Summary Totals

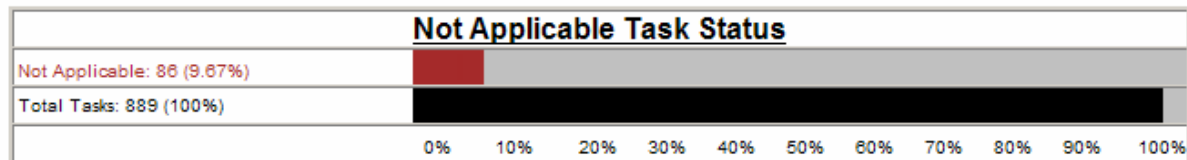
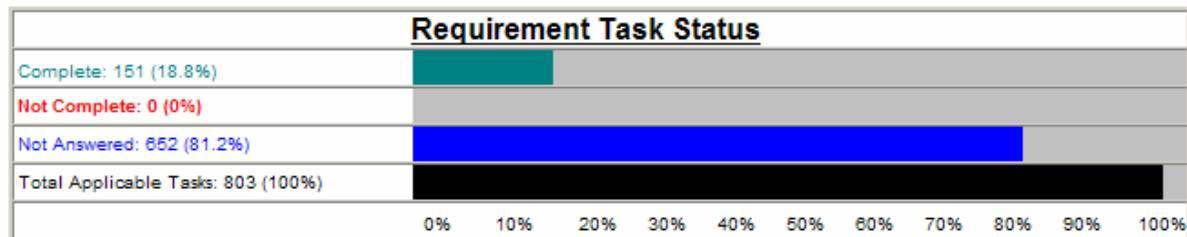
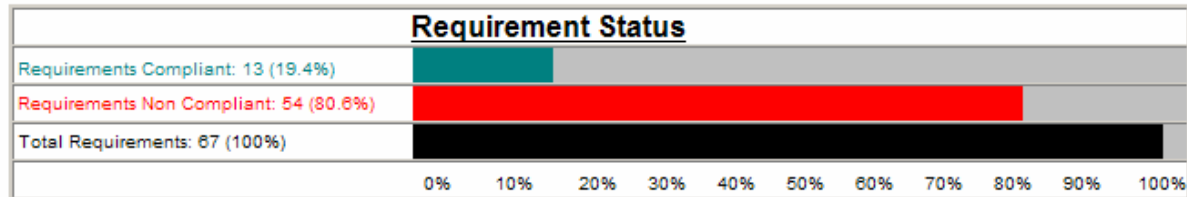
	% Compliant	% Not Compliant	# Requirements	# Compliant	# Not Compliant		
Requirement Status	19.4	80.6	67	13	54		
	% Complete	% Not Complete	% Not Answered	# Tasks	# Complete	# Not Complete	# Not Answered
Requirement Task Status	18.8	0	81.2	803	151	0	652
	% Non Applicable		Total # Tasks		# Non Applicable		
Non-Applicable Task Status	9.67		889		86		

Enhanced Gap Analysis Details

High Level Summary Report- Graphical

High Level Graphical Report

Organization Name and User	Report Date	HIPAA Rule
Training (Megan McCarron)	5/25/2005	Security Standards



Enhanced Gap Analysis Details

Detailed Requirement Report

1. Select the HIPAA Rule and report style
2. Click on **HTML Report** or **XLS Report**



The screenshot shows the 'Detailed Requirement Report' interface. At the top left is the 'HIPAA BASICS' logo. To the right, it says 'Subscriber : Training'. Below the logo are 'Log Off' and 'Menu' buttons. The main title 'Detailed Requirement Report' is centered, with a 'Help' button on the right. Under 'Select HIPAA Rule:', a dropdown menu shows 'Security Standards'. Below this, 'Include the following in Report:' is followed by a grid of checkboxes: 'Requirement Question', '# Tasks Complete', '# Tasks Not Complete', '# Tasks Not Answered', '# Tasks Not Applicable', and 'Requirement Note'. All are checked. At the bottom left, radio buttons for 'All', 'Compliant Requirements', and 'Non-Compliant Requirements' are shown, with 'All' selected. At the bottom center, two buttons 'HTML Report' and 'XLS Report' are highlighted with a red rectangle.

HIPAA BASICS™

Subscriber : Training

Log Off **Menu** **Detailed Requirement Report** **Help**

Select HIPAA Rule: Security Standards

Include the following in Report:

<input checked="" type="checkbox"/> Requirement Question	<input checked="" type="checkbox"/> # Tasks Complete	<input checked="" type="checkbox"/> # Tasks Not Complete
<input checked="" type="checkbox"/> # Tasks Not Answered	<input checked="" type="checkbox"/> # Tasks Not Applicable	<input checked="" type="checkbox"/> Requirement Note

☒ All ☐ Compliant Requirements ☐ Non-Compliant Requirements

HTML Report **XLS Report**

Enhanced Gap Analysis Details

Detailed Requirement Report Results

Detailed Requirement Report

Organization Name and User		Report Date		HIPAA Rule					
Training (Megan McCarron)		5/25/2005		Security Standards					
Gap ID: TRNG Test									
Lead User: Megan McCarron									
Req#	Req Question	Tasks% Complete	#Tasks Complete	#Tasks Not Complete	#Tasks Not Answered	#Tasks Not Applicable	Total #Tasks	Req Note	Compliance
107	A Security Management Process is implemented through policies and procedures to prevent, detect, contain, and correct security violations.	100	20	0	0	0	20	N	N
108	A Risk Analysis to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI was conducted (R).	100	19	0	0	0	19	Y	Y
109	A Risk Management Process that implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level is in place (R).	100	14	0	0	0	14	N	N
110	A Sanction Policy to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures has been developed (R).	100	7	0	0	0	7	Y	Y
111	Information System Activity Review procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports, are implemented (R).	-	0	0	0	15	15	Y	Y
112	A Security Official who is responsible for the development and implementation of the policies and procedures required by the Rule has been identified.	100	5	0	0	6	11	N	N
113	Policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information are implemented.	-	0	0	0	18	18	Y	Y
114	Procedures for the Authorization and/or Supervision of workforce members who work with electronic protected health information or in locations where it	-	0	0	0	9	9	Y	Y

Enhanced Gap Analysis Details

Summary

- You should now be able to:
 - Identify naming convention for Gaps
 - Assign Gaps to a HIPAA Rule
 - Tag Gaps for reporting
 - Describe importance of requirement notes
 - Generate enhanced reports at the Subscription level

Presentation Summary

- You should now be able to:
 - Identify use of HIPAA BASICS™
 - Describe user roles and responsibilities
 - Identify functionality of Report Admins at each level
 - Generate enhanced reporting as a Report Admin, Subscriber Administrator, and Lead User
 - Identify enhanced Gap Analysis details

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- <http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm>
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- <http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm> to subscribe to the TMA Privacy Office E-News
- HIPAA Service Privacy/Security Representatives